

An das

Bundesministerium für Verkehr, Innovation und Technologie
Radetzkystraße 2
A-1030 Wien

per E-Mail: stefan.vouk@bmvit.gv.at
klaus.parrer@bmvit.gv.at

Wien, am 13.03.2017

ISPA STELLUNGNAHME BETREFFEND DEN ENTWURF DER VERORDNUNG ÜBER PRIVATSPHÄRE UND ELEKTRONISCHE KOMMUNIKATION (E-PRIVACY VO)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Verkehr, Innovation und Technologie (BMvit) zum Entwurf der Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy VO) wie folgt Stellung zu nehmen:

Einleitend möchte die ISPA festhalten, dass die Entscheidung der Kommission begrüßt wird, durch das Rechtsinstrument der Verordnung eine einheitliche Rechtslage in den Mitgliedstaaten zu schaffen. Die ISPA ist jedoch der Ansicht, dass die in dem Entwurf enthaltenen Verweise auf die Richtlinie über den europäischen Kodex für die elektronische Kommunikation als ein noch nicht in Kraft getretenes Rechtsinstrument die Analyse erschweren und Unsicherheit schaffen. Zudem entspricht die Ausweitung des Anwendungsbereichs auf juristische Personen nicht einer Harmonisierung mit der DSGVO und ist somit nicht nachvollziehbar. Ferner fordert die ISPA, dass die Voraussetzungen zur Datenverarbeitung dem ausgereiften System der DSGVO folgen und hinsichtlich der Öffnungsklausel in Art 11 auf die beschränkte Zulässigkeit der Vorratsdatenspeicherung verwiesen wird, um der Rechtsprechung des EuGH Rechnung zu tragen und zukünftige Unsicherheiten in diesem Bereich hintan zu stellen. Zudem macht die ISPA darauf aufmerksam, dass eine alle sechs Monate notwendige Erinnerungsverpflichtung eine unverhältnismäßige Beeinträchtigung von Kommunikationsdienstbetreibern gegenüber anderen Unternehmen schafft. Außerdem verunmöglichen die Bestimmungen zur Aufnahme von Daten in Online-Verzeichnisse den Fortbestand dieser Dienstleistung und schaffen eine erhebliche Benachteiligung gegenüber anderen Diensten der Informationsgesellschaft, die ein gezieltes Auffinden von Inhalten im Netz ermöglichen. Im Sinne einer möglichst substanziellen Regelung spricht sich die ISPA für eine Streichung der technisch überholten Artikel 12 und 14 aus. Darüber hinaus ist die ISPA der Ansicht, dass durch den Entwurf Direktmarketingmaßnahmen unverhältnismäßig beschränkt werden und es eines differenzierteren Pönalensystems bedarf. Außerdem muss der Zeitpunkt des In-Kraft-Tretens jedenfalls eine entsprechende Umsetzungsfrist für Unternehmen berücksichtigen.

1) Verweise auf ein noch nicht in Kraft getretenes Rechtsinstrument erschweren Analyse und Vorbereitung

Einleitend möchte die ISPA festhalten, dass die Entscheidung der Kommission, das Rechtsinstrument der Verordnung zu wählen begrüßt wird, da auf diese Weise die Harmonisierung des Datenschutzstandards in den einzelnen Mitgliedstaaten gefördert werden kann. Dadurch ist insbesondere auch Telekom-Unternehmen geholfen, welche in mehreren Mitgliedstaaten am Markt tätig sind. Diese können nunmehr die gleichen Produkte in den einzelnen Mitgliedstaaten anbieten ohne dass zusätzliche Kosten für eine jeweils spezifische technische Adaptierung anfallen.

Die ISPA anerkennt zudem das Bestreben der Kommission, im Rahmen der Digital-Single-Market (DSM-) Strategie, ein möglichst homogenes System zu schaffen, weswegen in den Definitionen des vorliegenden Entwurfs in Art 4 auf die Begriffsbestimmungen insbesondere der Datenschutzgrundverordnung (DSGVO) aber auch auf jene der Richtlinie über den Wettbewerb auf dem Markt für Telekommunikations-Endgeräte (2008/63/EG) sowie auch auf einige Begriffe der Richtlinie über den europäischen Kodex für die elektronische Kommunikation (ECC) verwiesen wird. Hinsichtlich letzterer ist es jedoch problematisch, dass von dieser selbst erst ein Entwurf vorliegt, der von der Kommission im September 2016 präsentiert wurde.

Nach derzeitigem Stand wird es einen Beschluss über diese Richtlinie nicht vor Ende 2018 – und damit über ein halbes Jahr nach dem geplanten In-Kraft Treten der E-Privacy VO - geben. Ein solcher Verweis auf ein noch selbst der Abstimmung unterliegendes Rechtsinstrument ist ungewöhnlich und schafft eine Unsicherheit in der Analyse. Da es sich dabei um wesentliche Begriffsbestimmungen wie etwa „elektronischer Kommunikationsdienst“ handelt wäre eine nachträgliche Änderung der Begriffsbestimmungen des ECC auch gravierend für die Anwendung der E-Privacy VO. Um den Entwurf richtig einschätzen zu können bzw. es Unternehmen zu ermöglichen bereits vorzeitig Planungen für eine konforme Umsetzung zu tätigen soll daher die Schaffung einer solchen, nicht zwingend notwendigen Unsicherheit vermieden werden.

Nach Ansicht der ISPA ist es rechtlich nicht möglich, dass ein bereits in Kraft getretenes Rechtsinstrument im Rahmen der Definitionen auf ein anderes, noch nicht in Kraft befindliches – bzw. mit hoher Wahrscheinlichkeit auch noch nicht beschlossenes – Rechtsinstrument verweist.

Die ISPA fordert daher, die Definitionen in Artikel 2 Z 1, 4, 5, 6, 7, 14 bzw. 21 des Entwurfs des ECC, wortgleich in den Entwurf der E-Privacy VO zu übernehmen. Nach In-Kraft Treten des ECC wären diese Definitionen zwar möglicherweise redundant und könnten – auch um das Fortbestehen des homogenen Systems zu sichern – durch einen Verweis im Zuge einer Novelle ersetzt werden. Zuvor jedoch ist es zwingend erforderlich, diese Begriffsbestimmungen auch in die E-Privacy VO aufzunehmen.

2) Der sachliche Anwendungsbereich muss klarer formuliert werden

Wie den Ausführungen der Kommission auf Seite 1 der beiliegenden Begründung zu entnehmen, ist einer der Gründe für die Überarbeitung der E-Privacy VO die Miteinbeziehung von Over-The-

Top Kommunikationsdiensten (OTTs) welche im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst werden. Die ISPA begrüßt diese Bestrebungen da auf diese Weise auch ein level-playing field zwischen den unterschiedlichen Anbietern elektronischer Kommunikationsdienste geschaffen wird.

Die entsprechenden Ausführungen zum sachlichen Anwendungsbereich in Artikel 2 sind jedoch irreführend. So wird in lit c leg cit. ausgeführt, die Verordnung gelte nicht für „*elektronische Kommunikationsdienste, die nicht öffentlich zugänglich sind*“ in der englischen Version lautet die Bestimmung „*Electronic communication services which are not publicly available*“.

Die ISPA geht davon aus, auch aufgrund der Ausführungen in ErwG 13, dass die Kommission sich dabei auf Kommunikationsdienste beziehen möchte, die von der allgemeinen Öffentlichkeit nicht genutzt werden können/dürfen, etwa Kommunikation über unternehmens- bzw behördeninterne Netze. Die Formulierung „nicht öffentlich zugänglich“ würde jedoch auch die Auslegung erlauben, es seien von der Verordnung solche Kommunikationsdienste nicht umfasst, für die eine eigene Anmeldung erforderlich ist, was wiederum beinahe alle Dienste der Informationsgesellschaft ausschließen würde.

Da dies nicht im Sinne der Schaffung einheitlicher Datenschutzstandards erscheint, fordert die ISPA daher eine Klarstellung insbesondere der missverständlichen Formulierung in der deutschen Fassung der Verordnung, und eine Umformulierung in „*elektronische Kommunikationsdienste die der Öffentlichkeit nicht zugänglich/verfügbar sind*“.

3) Die Ausweitung des Anwendungsbereichs auf juristische Personen entspricht nicht der Harmonisierung und ist nicht nachvollziehbar

Gemäß Art 1 sollen vom Anwendungsbereich der Verordnung auch juristische Personen erfasst sein. Hierzu führt die Kommission in Erwägungsgrund 3 aus „*elektronische Kommunikationsdaten können Informationen über juristische Personen wie Geschäftsgeheimnisse oder andere sensible Informationen offenlegen, die einen wirtschaftlichen Wert haben*“ weshalb „*der Anwendungsbereich auch auf juristische Personen ausgedehnt werden [sollte]*“.

Entsprechende Überlegungen zur Miteinbeziehung von juristischen Personen wurden bereits zur Datenschutzgrundverordnung getroffen, jedoch wurde erkannt, dass die Interessen juristischer Personen bereits ausreichend durch wettbewerbsrechtliche sowie strafrechtliche Bestimmungen gewahrt werden. Eine Miteinbeziehung juristischer Personen nur in die E-Privacy Verordnung, nicht jedoch in die Datenschutzgrundverordnung würde zu einer evidenten Schlechterstellung von Betreibern von Kommunikationsdiensten gegenüber anderen Unternehmen führen.

Jedenfalls genießen juristische Personen aber nur hinsichtlich Art 7 u 8 GRC die gleichen Grundrechte wie natürliche Personen. Daraus folgt, dass selbst wenn die Kommission entgegen den Ansichten der ISPA zu dem Ergebnis gelangt, eine Miteinbeziehung juristischer Personen in

den Anwendungsbereich notwendig wäre, eine solche jedenfalls nur für Art 5 des vorliegenden Entwurfs im Lichte der Grundrechte gerechtfertigt erscheint.

4) Die Voraussetzungen zur Datenverarbeitung sollen der DSGVO folgen

Die Datenschutzgrundverordnung bietet in Artikel 5ff ein abgestuftes und flexibles System zur Datenverarbeitung welches versucht auf die verschiedenen involvierten Interessen der Beteiligten einzugehen und dabei die Grundrechte zu wahren. Hierzu werden zum Einen in Art 6 taxative Gründe – die Einwilligung der betroffenen Person sowie sechs weitere - zur gerechtfertigten Verarbeitung personenbezogener Daten aufgeführt. Zum Anderen werden durch besondere Bestimmungen etwa zur Verarbeitung sensibler Daten (Verarbeitung besonderer Kategorien personenbezogener Daten) Schranken gesetzt. Zusätzlich hat der Verantwortliche eine Datenschutz-Folgeabschätzung durchzuführen sofern die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte.

Diese risikobezogene Herangehensweise stellt anders als die im Datenschutz traditionelle rechtsbezogene Folgeabschätzung nicht direkt auf die Verletzung des Grundrechts ab, sondern auf Risikomanagement. Je höher das Risiko ist, durch den Datenverarbeitungsprozess gegen die Bestimmungen der DSGVO zu verstoßen, desto höher ist die Wahrscheinlichkeit für die Verletzung von Grundrechten zu sehen.

Im Rahmen der Folgeabschätzung müssen Unternehmen die zur Bewältigung der Risiken und geplanten Abhilfemaßnahmen darlegen, durch die der Schutz der personenbezogenen Daten sichergestellt wird. Eine solche Maßnahme ist etwa die Pseudonymisierung der Daten. Auf diese Weise wird den Rechten und berechtigten Interessen der betroffenen Personen in angemessener Weise bereits hinreichend Rechnung getragen.

Im nunmehr vorliegenden Entwurf wird von diesem ausgereiften System jedoch abgegangen. Die Verarbeitung von Kommunikationsmetadaten soll gemäß Art 6 (2) nur zu Verrechnungszwecken, zur Sicherstellung des Quality of Service sowie mit Einwilligung der betroffenen Person oder gänzlich anonymisiert zulässig sein. Dies stellt eine massive Einschränkung gegenüber den Gründen in Art 6 DSGVO dar. Gemäß den Ausführungen der Kommission in Erwägungsgrund 2, können durch Kommunikationsmetadaten sehr sensible und persönliche Informationen offengelegt werden (beispielsweise angerufene Nummern, besuchte Websites, der geografischer Standort,...). Dies entspricht auch der Rechtsprechung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung¹. Die ISPA teilt die Ansicht, dass insbesondere auch Kommunikationsmetadaten, sensible Rückschlüsse auf das Privatleben zulassen und anerkennt auch den Grundgedanken der Kommission hinsichtlich Datenminimierung.

Zu Beachten dabei ist jedoch – und dies erkennt die Kommission auch in ihren Ausführungen - dass jedenfalls immer der jeweilige Kontext der verarbeiteten Daten zu betrachten ist. Nicht alle Kommunikationsmetadaten stellen für sich bereits grundrechtssensible Daten dar. Die Beurteilung,

¹ EuGH 16.5.2014, C-293/12, *Digital Rights Ireland*; EuGH 21.12.2016, C-203/15 *Tele2 Sverige*

ob durch deren Verarbeitung die Gefahr von Grundrechtsverletzungen bestehe, wäre bereits durch die Risiko-Folgeabschätzung in der DSGVO, die auch auf die Verarbeitung personenbezogener Kommunikationsmetadaten anwendbar ist, abgedeckt .

Da nach den Grundsätzen der E-Privacy VO aber unabhängig vom jeweiligen Kontext alle Kommunikationsmetadaten erfasst werden, würde dies unter Umständen zu dem Ergebnis führen, dass am Ende sensible Metadaten, die nicht von der E-Privacy VO erfasst sind, eher verarbeitet werden dürfen, als Kommunikationsmetadaten, obwohl diese aber wiederum keine sensiblen Rückschlüsse zulassen. Beispielsweise lassen sich durch Kundendaten die Supermärkte aus der Nutzung von Kundenkarten beziehen, zum Einen Standortdaten – in welchem Supermarkt die Person einkauft – sowie insbesondere das jeweilige Kaufverhalten ableiten. Dabei besteht dem Grunde nach ein ähnliches Risiko für sensible Rückschlüsse auf das Privatleben des Einzelnen wie bei Kommunikationsmetadaten. Jedoch ist in diesem Fall, sofern die risikobasierte Folgeabschätzung zu dem Ergebnis kommt, dass aufgrund der getroffenen Maßnahmen – etwa Pseudonymisierung – kein Risiko für Grundrechte besteht, die Verarbeitung zulässig.

Im Ergebnis wären also ähnlich risikoreiche Datenverarbeitungsprozesse nur unter unterschiedlichen Voraussetzungen zulässig, dies wäre systemwidrig und würde Telekom-Unternehmen ungerechtfertigt in ihrem wirtschaftlichen Fortkommen behindern. Ebenso würden die gleichen Daten – abhängig von der jeweiligen Technologie – unterschiedlichen Schutz erhalten. Dies wird etwa beim Vergleich der Verarbeitung von GPS-Daten, die von Diensten der Informationsgesellschaft verarbeitet werden und Netzstandortdaten, die von Telekom-Betreibern verarbeitet werden deutlich. Beide enthalten dieselbe Information über den Standort, werden jedoch unterschiedlich behandelt. Eine solche Unterscheidung steht der Schaffung eines einheitlichen Datenschutzes wie dieser von der Kommission angestrebt wird entgegen und unterläuft zudem das ebenfalls im Rahmen der DSM-Strategie propagierte „level-playing-field“.

Die ISPA ist der Ansicht, die DSGVO biete bereits ein aufgrund langer Verhandlungen ausgereiftes und abgestuftes System für die Verarbeitung personenbezogener Daten welches strengere Anforderungen setzt, je höher das Risiko für Grundrechtsverletzungen ist, das durch die Verarbeitung dieser Daten geschaffen wird. Dieser Ansatz wird von uns begrüßt und sollte auch für Telekom-Betreiber beibehalten werden.

Zudem erscheint es ob der hohen Anforderungen an eine informierte Einwilligung im Sinne der DSGVO² in der Praxis technisch kaum umsetzbar, vor jeder Verarbeitung von Kommunikationsmetadaten eine rechtskonforme Einwilligung der betroffenen Person einzuholen.

Die ISPA fordert daher, um eine Gleichbehandlung gleicher Daten sicherzustellen, eine Ausweitung der Gründe in Art 6 (2) entsprechend Art 6 DSGVO, zumindest jedoch die Aufnahme des „berechtigten Interesses“ analog zu Art 6 (1) f DSGVO. Zudem sollte auch Kommunikationsdiensten die Möglichkeit einer Risikofolgeabschätzung eingeräumt werden, da auf diese Weise ein flexibles System geschaffen wird durch welches zudem die Entwicklung von sicheren, grundrechtskonformen Datenverarbeitungsprozessen gefördert wird. Die ISPA geht davon aus, dass ein solches System keinesfalls zu einer Schlechterstellung der Nutzerinnen und

² Die E-Privacy VO verweist in Art 9 hinsichtlich der Einwilligungserfordernisse auf die DSGVO

Nutzer führen würde, da Telekom-Unternehmen bereits in der Vergangenheit über zahlreiche Daten verfügt haben, diese jedoch stets mit äußerster Sorgfalt behandelt haben weshalb gegenüber etablierten Betreibern auch ein Vertrauen seitens der Nutzerinnen und Nutzer besteht. Beispielsweise setzen sich Betreiber seit Jahren für eine rechtskonforme und auf das Notwendigste beschränkte Beauskunftung von Kundendaten gegenüber Behörden ein und haben in diesem Zusammenhang auch bereits zahlreiche Gerichtsverfahren geführt.

5) In die Öffnungsklausel in Art 11 soll eine Bestimmung zur Speicherung von Vorratsdaten aufgenommen werden um der Rechtsprechung des EuGH Rechnung zu tragen

Bereits 2014 entschied der Europäische Gerichtshof (EuGH), in der Rechtsache *Digital Rights Ireland*, dass die anlasslose Vorratsdatenspeicherung mit europäischen Grundrechten nicht zu vereinbaren sei. Ungeachtet dessen beschlossen einige Mitgliedstaaten anschließend jedoch weiterhin Gesetze zur Vorratsdatenspeicherung und beriefen sich dabei auf Art 15 der E-Privacy RL, der es Mitgliedstaaten unter bestimmten Voraussetzungen (etwa dem Schutz der öffentlichen Sicherheit) erlaubt, Rechte und Pflichten aus der Richtlinie, insbesondere hinsichtlich der Vertraulichkeit von Kommunikationsdaten und der verpflichteten Löschung, zu beschränken.

In der Rechtsache *Tele2 Sverige* hat der Europäische Gerichtshof jedoch klargestellt, Art 15 E-Privacy RL dürfe nicht dazu missbraucht werden, die Grundprinzipien der Richtlinie auszuhöhlen. EU-Mitgliedstaaten dürfen demnach keine allgemeine Verpflichtung zur Vorratsdatenspeicherung festlegen. Das Gericht hat zudem klargestellt, dass eine Verwendung von Vorratsdaten nur zur Bekämpfung schwerer, nicht aber bereits zur Bekämpfung einfacher Kriminalität legitim ist und der Zugang zu den Daten sowie Ausmaß, Art und Speicherdauer der Daten auf das absolut Notwendigste beschränkt werden müssen.

Im nunmehr vorliegenden Entwurf ist in Art 11 wiederum eine solche Öffnungsklausel enthalten. Bezüglich der legitimen Interessen, die eine Beschränkung der enthaltenen Rechte und Pflichten rechtfertigen können, wird auf die entsprechende Auflistung in Art 23 (1) DSGVO verwiesen. Es handelt sich dabei im Wesentlichen um die gleichen Gründe wie bisher. Den Ausführungen der Kommission auf Seite 3 der beiliegenden Begründung kann man entnehmen, dass offensichtlich bewusst keine eigene Bestimmung zur Vorratsdatenspeicherung aufgenommen wurde. Es wird dabei lediglich darauf verwiesen, dass es Mitgliedstaaten weiterhin frei steht, nationale Rahmen für die gezielte Vorratsdatenspeicherung zu schaffen solange diese mit der Rechtsprechung des EuGHs zur Auslegung der E-Privacy RL und der Grundrechtecharta vereinbar sind. Diese Ausführungen sind grundsätzlich jedoch redundant, da nationales Recht jedenfalls immer die Rechtsprechung des EuGHs sowie die Grundrechtecharta beachten muss.

Angesichts der bedenklichen Entwicklungen in zahlreichen Mitgliedstaaten, in welchen erneut eine umfassende Vorratsdatenspeicherung gefordert wird, spricht sich die ISPA jedoch für die Aufnahme einer eigenen Bestimmung aus, durch welche klargestellt wird, dass die Grundprinzipien der Verordnung – die Vertraulichkeit der Kommunikation sowie verpflichtende

Löschung von Kommunikationsdaten - durch die Anwendung der Öffnungsklausel in Art 11 nicht untergraben werden dürfen. Die ISPA schlägt vor, folgende Formulierung an Art 11 Abs. 1 anzuhängen:

Durch die Anwendung dieser Beschränkungen dürfen die in den Artikeln 5 bis 8 festgelegten Pflichten und Rechte jedoch nicht in ihrem Wesensgehalt untergraben werden und ist die Maßnahme sowohl zeitlich als auch sachlich auf das Notwendigste zu beschränken.

Dadurch soll der aktuellen Rechtsprechung des EuGH Rechnung getragen werden und auch der Rechtsicherheit geholfen werden. Zusätzlich soll in den Erwägungsgründen eine Erläuterung entsprechend den Ausführungen des EuGHs in der Rechtsache *Tele2 Sverige* aufgenommen werden in der dieser Grundsatz näher im Zusammenhang mit der Vorratsdatenspeicherung ausgeführt wird:

Nationale Regelungen, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht, sind durch die Anwendung der Öffnungsklausel nicht gerechtfertigt.

Damit soll kein neues Recht geschaffen werden sondern lediglich die bereits geltende – durch den EuGH mehrmals bestätigte – Rechtslage festgeschrieben werden, um in Zukunft derart grundrechtsverletzende Maßnahmen bereits von Beginn an deutlich zu unterbinden, ohne dass ein aufwendiges Verfahren bis zum europäischen Höchstgericht geführt werden muss.

6) Eine alle sechs Monate notwendige Erinnerungsverpflichtung schafft eine unverhältnismäßige Belastung für Unternehmen

Gemäß Art 9 (3) des Entwurfs, soll Endnutzern die Möglichkeit eingeräumt werden, ihre Einwilligung zur Verarbeitung elektronischer Kommunikationsdaten jederzeit widerrufen zu können. Dies entspricht Art 7 (3) DSGVO und wäre sohin in Zukunft ohnedies bereits erfasst.

Zusätzlich wird jedoch vorgesehen, dass Endnutzer vom Betreiber in regelmäßigen Abständen von sechs Monaten an diese Möglichkeit zum Widerruf erinnert werden müssen, solange die Verarbeitung andauert. Nähere Ausführungen – etwa zur technischen Ausgestaltung - werden jedoch sowohl in den Erwägungsgründen als auch in der Begründung verabsäumt.

Eine solche, in dermaßen kurzen Abständen widerkehrende Informationspflicht stellt eine große Belastung für die Unternehmen dar, da jeweils alle relevanten Datenverarbeitungsprozesse gesammelt werden müssen um diese Information dem Kunden geordnet zu übermitteln. Es ist nicht verständlich weshalb eine solche Belastung lediglich Telekom-Betreiber treffen soll, während in den allgemeinen Regelungen zum Widerrufsrecht in der DSGVO eine entsprechende Informationspflicht nicht vorgesehen ist.

Zudem ist fraglich, welcher Umfang dieser Informationspflicht tatsächlich zukommen soll, etwa ob über die Widerrufsmöglichkeit zu jedem einzelnen Datenverarbeitungsprozess zu informieren ist, oder ob für alle Prozesse eine gesammelte Information an den Kunden ausreicht.

Die ISPA spricht sich klar gegen eine solche Schlechterstellung von Telekom-Betreibern aus und fordert die ersatzlose Streichung des letzten Halbsatzes in Art 9 (3). Sofern dieser beibehalten wird, sollen in die Verordnung jedoch jedenfalls Ausführungen zur genaueren Ausgestaltung dieser Verpflichtung aufgenommen werden, da Unternehmen sonst in Gefahr laufen, sich den zum Teil immensen Pönalen auszusetzen. Ferner spricht sich die ISPA dafür aus, dass es sich jedenfalls um eine gesammelte Erinnerungsverpflichtung handeln solle.

7) Die technisch überholten Regelungen in Art 12 und Art 14 sollen ersatzlos gestrichen werden

Artikel 12 und 14 des Entwurfs enthalten technische Bestimmungen welche sich im Wesentlichen auf das Blockieren bestimmter Anrufe, die Rufweiterleitung sowie die Rufnummernanzeige beziehen. Diese Bestimmungen sind zum Teil aufgrund der technischen Ausgestaltung der Endgeräte überholt und damit redundant oder aber technisch nicht einwandfrei umsetzbar und daher auch bisher in Österreich bereits totes Recht.

Die Möglichkeit für den Anrufer seine Rufnummer zu unterdrücken um anonym zu bleiben (Art 12 Abs. 1 lit a) wird bereits heute standardmäßig in den meisten Endgeräten angeboten und erscheint es nicht notwendig, hierzu eine eigene Bestimmung aufzunehmen.

Andererseits verfügen heute bereits viele Endgeräte auch über die Funktion, bestimmte eingehende Anrufe (beispielsweise sämtliche mit unterdrückter Rufnummer) zu unterdrücken. Dadurch soll unter anderem Stalking-Opfern die Möglichkeit gegeben werden, Stalking-Anrufe zu unterdrücken. Die im Entwurf vorgesehene Verpflichtung des Betreibers, die Anrufe bereits im Netz des Angerufenen zu blockieren (vgl Art 12 Abs. 1 lit c bzw Art 14 lit a) ist damit ebenfalls technisch überholt und schafft lediglich unverhältnismäßigen Aufwand.

Zudem kann es gerade im internationalen Telefonverkehr vorkommen, dass bei einzelnen Stellen eine Rufnummer nicht mit übermittelt wird. Dies hätte sodann zur Folge, dass der Anruf netzseitig nicht durchgestellt wird, obwohl der Anrufende die Nummer ursprünglich mitgeschickt hat. Insbesondere auch angesichts der in der Verordnung vorgesehenen, hohen Strafdrohungen sollte daher von dieser Regelung abgegangen werden, da sie nicht einwandfrei umsetzbar ist.

Die weiteren Bestimmungen sind bereits im österreichischen Telekommunikationsgesetz (TKG) enthalten, jedoch handelt es sich dabei um totes Recht. Die vom Angerufenen veranlasste Unterdrückung der Rufnummernanzeige eingehender Anrufe (Art 12 Abs. 1 lit b) ist derzeit in § 104 Abs. 2 TKG geregelt wurde aber aufgrund des geringen Anwendungsbereichs (zB. Seelensorge) bisher nicht nachgefragt.

Auch die Bestimmungen zur Abstellung einer von einem Dritten veranlassten automatischen Anrufweitschaltung zur Endeinrichtung des Endnutzers (Art 14 lit b) war bereits bisher in § 105

TKG enthalten, jedoch gibt es hierzu keine automatisierten technischen Möglichkeiten für den Betreiber des betroffenen Endnutzers, da immer nur der Netzbetreiber des Veranlassers dazu in der Lage ist, die Rufnummernweiterleitung zu unterbinden. Bisher war die Bestimmung daher ebenfalls totes Recht.

Die ISPA regt daher an, insbesondere in Anbetracht des Grundgedankens einer möglichst substantziellen Regelung, sowohl Artikel 12 als auch Artikel 14 ersatzlos zu streichen.

8) Der Betrieb von Online-Verzeichnissen wird geradezu verunmöglicht

Gemäß der derzeitigen Rechtslage, sind Telekom-Betreiber durch die Richtlinie 98/10/EG, Artikel 6 Absatz 3 und § 18 (1) Z. 4 TKG, dazu verpflichtet, vergebene Telefonnummern samt Teilnehmerdaten an die Herausgeber betreiberübergreifender Telefonverzeichnisse zu übermitteln. Die Einholung der Zustimmung der betroffenen Person obliegt derzeit dem Telekom-Betreiber im Zuge der Vertragserstellung mit dem jeweiligen Teilnehmer.

Im nun vorliegenden Entwurf ist in Art 15 vorgesehen, dass der Anbieter des Online-Verzeichnisses selbst die Einwilligung von allen natürlichen Personen vorab einzuholen hat („*opt in*“) und zudem die kostenfreie Möglichkeit zur Korrektur oder Löschung gegeben sein muss. Zudem müssen Informationen über die vorhandenen Suchfunktionen bereitgestellt werden. Juristische Personen soll die Möglichkeit eingeräumt werden, der Aufnahme von auf sie bezogenen Daten zu widersprechen („*opt out*“), bzw diese zu korrigieren oder zu löschen.

Durch die Übertragung der Verantwortung zur Einholung der Einwilligung auf die Anbieter der Online-Verzeichnisse, wird diesen die weitere Herausgabe von Verzeichnissen in der Praxis verunmöglicht, da es den Betreibern nicht möglich ist selbst an alle Nutzerinnen und Nutzer – insbesondere auch aufgrund der im Entwurf enthaltenen verschärften Bestimmungen zur unerbetenen Kommunikation – heranzutreten. Ohne Möglichkeit einer Kontaktaufnahme ist die vorgeschlagene *opt-in* Regelung nicht zu bewerkstelligen und kommt de facto einem Verbot von elektronischen Telefonverzeichnissen gleich.

Daneben ist fraglich, ob betroffenen Personen nicht bereits durch Anwendung von Art 17 DSGVO (Recht auf Löschung – *opt out*) ein ausreichend ausgereiftes Recht zur Verfügung steht, welches bereits in Abwägung der Interessen der involvierten Parteien, insbesondere dem Datenschutz und der Privatsphäre des Einzelnen sowie dem allgemeinen Recht auf Informationszugang entworfen wurde. Eine eigens verschärfte Regelung für Online-Verzeichnisse in Art 15 E-Privacy VO erscheint damit hinfällig, da auch hier dieselben Interessen involviert sind.

Insbesondere muss in diesem Zusammenhang darauf verwiesen werden, dass auch weitere Diensten der Informationsgesellschaft ein gezieltes Auffinden von Inhalten im Netz ermöglichen und ebenfalls die Möglichkeit zur Suche nach natürlichen Personen inklusive deren Kontaktdaten bieten. In Auslegung des sachlichen Anwendungsbereichs der Verordnung ergibt sich jedoch, dass solche Dienste nicht von den Bestimmungen umfasst wären. Dies hätte zur Folge, dass für diese jedenfalls nur eine *opt-out* Regelung nach Art 17 DSGVO gelten würde. Auf diese Weise werden insbesondere kleine, lokale Verzeichnisanbieter benachteiligt und im Endeffekt lediglich diesen

ihre unternehmerische Tätigkeit verunmöglicht ohne dabei den Grundrechtsschutz für Nutzerinnen und Nutzer tatsächlich zu erhöhen.

Wie bereits in Punkt 3 ausgeführt, entspricht die Miteinbeziehung von juristischen Personen in den Anwendungsbereich der E-Privacy Verordnung nicht einer Harmonisierung der Datenschutzstandards und ist daher auch dieser Punkt kritisch zu sehen. In Erwägungsgrund 14 der DSGVO wird der Anwendungsbereich für juristische Personen explizit verneint und ferner ausgeführt, dass auch die Kontaktdaten juristischer Personen nicht vom Schutzbereich umfasst seien.

Die ISPA fordert daher die ersatzlose Streichung von Art 15, da nach Ansicht der ISPA durch die Anwendung von Artikel 17 DSGVO auch auf Verzeichnisanbieter - sofern es sich bei den jeweiligen Daten um personenbezogene Daten handelt - dem Datenschutz und der Privatsphäre der betroffenen Personen ausreichend Rechnung getragen wird. Die Aufnahme einer eigenen Bestimmung für juristische Personen erscheint im Vergleich zur DSGVO systemwidrig und ist daher abzulehnen.

9) Die Anwendung von Direktmarketing wird unverhältnismäßig eingeschränkt

Zunächst begrüßt die ISPA den Umstand, dass im Entwurf eine Definition zu Direktmarketing enthalten ist, da eine solche bisher – etwa in der DSGVO – fehlt.

Direktmarketing als solches wird zwar in der DSGVO nicht ausdrücklich erwähnt, Erwägungsgrund 47 verweist jedoch explizit darauf, dass es sich dabei um ein berechtigtes Interesse im Sinne von Art 6 (1) lit f DSGVO handeln könne. Die Frage der Zulässigkeit und des Umfangs der Zulässigkeit von Direktwerbung blieb demnach offen und müsste im Einzelfall beurteilt werden. Daraus folgt, dass der Gesetzgeber sich offensichtlich nicht festlegen wollte zu diesem Thema, da es zu vielseitig und umstritten für eine allgemeine Regelung in der Verordnung wäre.

Umso erstaunlicher erscheint es nun, dass eine Bestimmung zu Direktmarketingmaßnahmen Eingang in die E-Privacy Verordnung gefunden hat. In Art 16 des Entwurfs, wird vorgesehen, dass diese grundsätzlich lediglich mit Einwilligung der betroffenen Person zulässig ist. Absatz 2 sieht darüber hinaus die Möglichkeit zur Nutzung von E-Mail-Kontaktangaben im Rahmen einer bestehenden Kundenbeziehung vor, sofern damit ähnliche Produkte oder Dienstleistungen angeboten werden. Fraglich bleibt dabei jedoch, ob davon etwa auch die Produkte von ausländischen Konzernschwestern erfasst wären.

Durch die Aufnahme dieser Bestimmung wird ein ursprünglich der Einzelfallabwägung überlassener Bereich plötzlich massiv eingeschränkt. Da der Begriff der Direktwerbung im Sinne der Verordnung jegliche schriftliche oder mündliche Werbung über elektronische Kommunikationsdienste umfasst, kann Direktwerbung als berechtigtes Interesse des Betreibers gemäß der DSGVO nur noch für das Versenden per Briefpost bestehen. Dieses Ergebnis kann jedenfalls nicht im Sinne einer zukunftsorientierten Regelung sein und erscheint eine solche Einschränkung gegenüber den Grundsätzen der DSGVO auch nicht gerechtfertigt.

Aus diesen Gründen fordert die ISPA die ersatzlose Streichung der Bestimmungen zu Direktmarketingmaßnahmen da diese allgemein dem Anwendungsbereich der DSGVO unterliegen sollten.

Sofern die Bestimmung erhalten bleibt besteht jedoch keine sachliche Begründung, weswegen bei aufrehtem Vertrag gemäß Abs. 2 lediglich E-Mail Kontaktdaten, nicht jedoch andere Kanäle wie SMS, Instant Messaging und Ähnliches genutzt werden dürfen, speziell da diese Dienste im restlichen Teil des Entwurfs gleichgestellt werden, bzw. eine solche technische Gleichstellung sogar einer der Grundgedanken hinter der Überarbeitung der E-Privacy Richtlinie war. Insbesondere die entsprechenden Ausführungen in ErwG 33 sind widersprüchlich da darin einerseits betont wird, dass es aus Gründen der Rechtssicherheit notwendig sei, dass alle Kommunikationskanäle gleich behandelt werden, nur um anschließend wiederum lediglich E-Mail-Kontaktangaben herauszuheben. Zudem wird auch diese Ausnahme wiederum durch die Verpflichtung zur Einräumung eines Widerspruchsrechts bereits bei Erhalt der Kontaktangaben erheblich eingeschränkt da dies in der Praxis nur schwierig umsetzbar ist. Die ISPA ist der Ansicht dass, wenn bereits die Möglichkeit zur Direktwerbung erheblich eingeschränkt wird, zumindest die Ausnahmebestimmung praxisnah ausformuliert sein sollte. Eine solche *opt-out* Möglichkeit sollte daher erst im Zeitpunkt des Versands der Werbung verpflichtend vorgeschrieben werden, damit wäre jedenfalls auch der Hinweispflicht zum möglichen Widerspruch in der DSGVO (Art 21 Abs. 4 DSGVO) entsprochen.

In Bezug auf die Öffnungsklausel hinsichtlich einer Anwendung auf juristische Personen in Abs. 5 sei wiederum auf die kritischen Ausführungen in Punkt 3 verwiesen. Zudem wäre jedoch angesichts des Verweises auf Abs. 1 klarzustellen, ob wie die Formulierung „sending direct marketing communications“ in der englischen Sprachversion nahelegt, hiervon bewusst Direktanrufe ausgenommen sind, oder ob wie der deutschen Formulierung „Direktwerbung über elektronische Kommunikationsdienste an Endnutzer richten“ zu entnehmen sämtliche Direktwerbung im Sinne der Definition in Art 4 (3) lit g umfasst sein soll.

10) Die vorgesehenen Pönalen sind überschießend und für klein- und mittelgroße Unternehmen existenzbedrohend

Zunächst möchte die ISPA anmerken, dass Art 23 (1) offensichtlich versehentlich auf Kapitel VII DSGVO (Zusammenarbeit und Kohärenz) verweist. Gemeint ist aber wohl Kapitel VIII (Rechtsbehelfe, Haftung und Sanktionen).

Analog zu den Strafbestimmungen der DSGVO, sind auch die Pönalen in der E-Privacy Verordnung äußerst hoch bemessen und lediglich mit den Geldbußen im Kartellrecht vergleichbar. Zwar erkennt die ISPA, dass hierdurch bereits von Anfang an ein Abschreckungseffekt geschaffen werden soll, der auch gegenüber großen Unternehmen wirksam ist. Für kleine und mittelgroße Unternehmen (KMUs) sowie Start-Ups wäre die Verhängung einer solchen Pönale – für die zudem auch keine vormalige Verwarnung vorgesehen ist - jedoch jedenfalls existenzbedrohend. Diese sind es jedoch, welche digitale Innovationen vorantreiben. Drohende Pönalen in Höhe von bis zu

EUR 10 bzw. 20 Mio. würden dazu führen, dass KMUs und Start-Ups angesichts des Haftungsrisikos gänzlich abgeschreckt, weiterhin innovativ tätig zu sein. Obwohl damit die Strafbestimmungen insbesondere zur Abschreckung auch größerer Unternehmen dienen sollen, wird am Ende vor allem der Wettbewerb verringert, da KMUs und Start-Ups ob des Risikos eher vom Markt verschwinden werden.

Die ISPA spricht sich daher deutlich gegen die hohen Strafandrohungen bereits bei kleineren Verstößen aus, und fordert eine differenzierte Abstufung der Strafmaße bereits in der Verordnung. Hiedurch soll eine Absicherung gegen existenzbedrohende Strafen für KMUs verankert werden um dies nicht gänzlich dem Ermessensspielraum der zuständigen Behörde zu überlassen.

11) Der Zeitpunkt des In-Kraft-Tretens sollte auch eine entsprechende Umsetzungsfrist für Unternehmen berücksichtigen

Wie bereits unter Punkt 1 ausgeführt plant die Kommission, dass E-Privacy VO und DSGVO gemeinsam, am 25.05.2018 in Kraft treten. Wie das Gesetzgebungsverfahren zur DSGVO jedoch gezeigt hat, können die Verhandlungen, aufgrund der sehr stark divergierenden Interessen der involvierten Parteien einen erheblichen Zeitraum in Anspruch nehmen. Sofern – und dies liegt durchaus nahe – auch das Gesetzgebungsverfahren zur vorliegenden Verordnung ähnlich viel Zeit in Anspruch nimmt, würde dies dazu führen, dass das finale Dokument erst wenige Monate vor dem geplanten In-Kraft-Treten vorliegen würde. Aufgrund der direkten Anwendbarkeit der Verordnung, würden Unternehmen aber umgehend zur Einhaltung der Bestimmungen verpflichtet sein und sich andernfalls Strafdrohungen aussetzen.

Die ISPA fordert daher, obgleich des durchaus verständlich gewählten Zeitpunkts zum gemeinsamen In-Kraft-Treten der beiden Rechtsinstrumente, dass sobald ersichtlich wird, dass ein finaler Text nicht zumindest ein Jahr vor In-Kraft-Treten vorliegen werde, ein späterer Zeitpunkt festgelegt wird. Denn ohne entsprechende Umsetzungsfrist für Unternehmen kann es zu keiner ordnungsgemäßen Implementierung der neuen Datenschutzstandards kommen.

Für Rückfragen oder weitere Auskünfte stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria



Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.